PRIVACY IMPACT ASSESSMENT (PIA)

1. Department of Defense Component

Department of the Army, Director of the Army Staff

2. Name of Information Technology System

Senior Leader Development Management System (SLDMS)

3. Budget System Identification Number (SNAP-IT)

9990

4. System identification Number (IT Registry/Defense IT Portfolio Repository (DITPR))

7973

5. IT Investment Unique Identifier

NA

6. Privacy Act System of Records Notice Identifier

A0680-31a AHRC, Officer Personnel Management Information System (OPMIS),

7. OMB Information Collection Requirement Number and Expiration Date

NA

8. Type of Authority to Collect Information

5 U.S.C 301, Departmental Regulations,
10 U.S.C 3013, Secretary of the Army,
E.O. 9397 (SSN)

9. Summary of the System

The Senior Leader Development Management System (SLDMS) is knowledge based succession management system that utilizes data collected from other Army Human Resource Systems of Record to leverage the talents, skills and experiences of the Army Senior Leaders to place the right officer in the right position at the right time. SLDMS is divided into two main systems. The first is the General Officer Resource Management Systems (GORMS) and is primarily used to provide the Chief of Staff, Army real-time data and information (through the General Officer Management Office) on the roughly 350 General Officers on Active Duty. Functions include slate management, adverse information tracking, and peer and advisory evaluation. Slate management refers to the identification of possible successors to the incumbent in one or many General Officer positions. As General Officers are routinely in the public eye, they are more scrutinized when they are selected for promotion or choose to retire. SLD maintains liaison with various other Army and DoD Agencies to collect reports from these agencies on adverse information on General Officers. The General Officers are afforded the opportunity to respond to the various allegations. The allegation and the officer's response determine if the favorable personnel action will be completed. The Peer and Advisory is an on-line survey to Active Duty General Officers conducted yearly by the direction of the Chief of Staff, Army. The purpose of the Peer and Advisory is to provide anonymous peer review and feedback, as well as provide information to the Chief of Staff, Army on the status of his General Corps.

The second half of the system is the Colonels Management System (CMS). CMS was designed off the GORMS model and also serves as a succession management system. The main modules of the CMS are the Developmental Opportunities Module (DOM), the Peer Developmental Feedback (PDF) Survey and the Adverse Module. For the supported Colonel population the DOM serves as the listing of available positions for the next Calendar Year. For the Senior Leader Development Office, the DOM serves as the basis for operations of the organization and is the slate management/succession management tool to link the officer's skills, talents and experiences with the requirements of current or future positions. The Peer Developmental Feedback (PDF) survey operates similar to the General Officer Peer and Advisory, as it uses the same questions. The results of the PDF Survey are shared with the officer that received survey data. The Adverse tracking module works under the similar process of the adverse module of General Officers.

10. Identifiable Information Collected, its Nature and Source

Name, nickname, social security number, gender, race/ethnicity, date of birth, personal and business email addresses, personal and duty physical addresses, security clearance level and status, marital status, spouse name, dependant name, exceptional family member enrollment, assignment history, talents, skills, experiences, education, training, peer evaluation, adverse information relating to conduct, awards, decorations, source of commission, year group, dates of rank, languages, and military career field. Data is collected from existing personnel database systems and from the individual during personal interviews or data entry.

11. Method of Information Collection:

Some personal information is provided by the individual record subject through completion of on-line and paper forms and via personal interviews. Most basic service information is acquired from other Army personnel database systems.

12. Purpose of collection and How Identifiable Information/Data will be Used:

Most personally identifiable information is collected through data imports from existing Army personnel systems. Additional information is collected directly from the officer during interviews or on-line completion of forms. Personally identifiable information is used by SLD for the assignment selection and slating process. Name and basic military branch are used by other authorized system users to begin the Peer and Advisor or Peer Development Feedback surveys. "Go by" names, email address, home address and spouse information is used in generating thank you and congratulatory notes from the Chief of Staff, Army and Vice Chief of Staff, Army. Dependent names are collected for General Officers for the purpose of personalizing letters and notes. Adverse information is tracked and considered during the promotion and assignment process.

13. Does system create new data about individuals through aggregation:

The system does not derive or create any new data about individuals through aggregation.

14. Internal and External Information/Data Sharing:

Information will be available to authorized users with a need to know in order to perform official government duties. Internal DoD agencies that would obtain access to PII in this system, on request to support of an authorized investigation or audit, may include DoD IG, DCIS, DFAS, Army Staff Principals in the Chain of Command, DAIG, AAA, USACIDC, INSCOM, PMG and ASA FM&C. In addition, the DoD blanket routine uses apply to this system.

15. Opportunities individuals will have to object to the collection of information in identifiable form

Personal data is voluntarily given by the individual and collected via electronic forms, manual forms or interview. Forms requesting privacy information contain an applicable privacy statement. Individuals are advised via interview that all data provided is optional, but failure to provide may result in incomplete data for succession management or personalized letters from the CSA or VCSA. Privacy Act Advisory Statements are available upon log-in to the system. The basic database record is constructed based on automatic data feed from Army personnel systems upon promotion and the individual record subject is not involved in that process.

16. Information Provide to the Individual, the Format, and the Means of Delivery

The Privacy Act Advisory statement is provided to the individual as additional data is collected. Data is also imported from other Army Personnel Systems. The Privacy Act Advisory statement is also provided to the individual on the SLDMS website (an integral portion of the application). Individuals are furnished Privacy Act Advisory statements as they appear in various applications in other portions of the website. Individuals are presented a summary of the data that they have provided.

17. Administrative/business, physical, and technical process that data controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form

This system has a current certification and accreditation, having met all Army system security requirements. The system resides within a secured military/federal facility with 24 hour security guards, alarm systems and secured offices within the facility. Personnel accessing government computer information systems are required to undergo and receive at a minimum a favorable National Agency Check. The users include Active Duty Military, Federal Civil Service personnel and authorized contractors working directly for the Senior Leader Development Office that have a need to know in order to perform official government duties. Both contractor and government employees may have access requirements and are limited to specific or general information in the computing environment. The System Administrator defines specific access requirements dependent upon each user's role. Each application within the system may further restrict access via application-unique permission controls. Currently, only system users have the capability to connect to the system. Each authorized user must enter their appropriate AKO Username and password before being authorized access to the resources. AKO provides immediate monitoring and disables accounts that may be compromised; AKO's current policies enforce complex user passwords. Additionally, there is a monthly audit to remove roles and permissions for users that no longer require access. The system is maintained in a manner that provides network intrusion detection, is located behind an appropriately configured firewall and is regularly updated to adhere to Information Assurance Vulnerability Alerts (IAVA's) and Security Technical Implementation Guides (STIG's) as they are released. Files transferred across the Internet/NIPRNet are encrypted via Secure Sockets Layer (SSL).

18. Potential privacy risks regarding the collection, use, and sharing of the information, dangers in providing notices or opportunities to object/consent to individuals; risks posed by the adopted security measures

Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal. There are no risks in providing individuals the opportunity to object or consent.

19. Classification and Publication of Privacy Impact Assessment

The data in the system is For Official Use Only. The PIA may be published in full.